15 November 1999
DRAFT
INTERNATIONAL SAFE HARBOR PRIVACY PRINCIPLES
ISSUED BY THE U.S. DEPARTMENT OF COMMERCE

The European Union's comprehensive privacy legislation, the Directive on Data Protection (the Directive), became effective on October 25, 1998. It requires that transfers of personal data take place only to non-EU countries that provide an "adequate" level of privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Community. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation. Given those differences, many U.S. organizations have expressed uncertainty about the impact of the EU-required "adequacy standard" on personal data transfers from the European Community to the United States.

To diminish this uncertainty and provide a more predictable framework for such data transfers, the Department of Commerce is issuing this document and Frequently Asked Questions (the principles) under its statutory authority to foster, promote, and develop international commerce. The principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of "adequacy" it creates. Because the principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate.

Decisions by organizations to qualify for the safe harbor are entirely voluntary, and organizations may qualify for the safe harbor in different ways. Organizations that decide to adhere to the principles must comply with the principles in order to obtain and retain the benefits of the safe harbor and publicly declare that they do so. For example, if an organization joins a self regulatory privacy program that adheres to the principles, it qualifies for the safe harbor. Organizations may also qualify by developing

their own self regulatory privacy policies provided that they conform with the principles. Where in complying with the principles, an organization relies in whole or in part on self regulation, its failure to comply with such self regulation must also be actionable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts.

Organizations subject to a statutory, regulatory, administrative or other body of law (or body of rules issued by national securities exchanges, registered securities associations, registered clearing agencies, or a Municipal Securities Rule-making Board) that effectively protects personal privacy may assure safe harbor benefits by self-certifying to the Department of Commerce or its nominee. In all instances, safe harbor benefits are assured from the date on which each organization wishing to qualify for the safe harbor self-certifies to the Department of Commerce or its nominee its adherence to the principles in accordance with the guidance set forth in the Frequently Asked Question on Self Certification.

Adherence to these principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations. Organizations may wish for practical or other reasons to apply the principles to all their data processing operations, but they are only obligated to apply them to data transferred after they enter the safe harbor. To qualify for the safe harbor, organizations are not obligated to apply these principles to personal information in manually processed filing systems. Organizations wishing to benefit from the safe harbor for receiving such information from the EU must apply the principles to any such information transferred after they enter the "safe harbor."

Organizations will also be able to provide the safeguards necessary under Article 26 of the Directive if they include the principles in written agreements with parties transferring data from the EU for the substantive privacy provisions, once the other provisions for such model contracts are authorized by the Commission and the Member States.[(1)] Personal data and personal information are data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S.

organization from the European Union, and recorded in any form.

NOTICE: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure, where the organization is using or disclosing it for a purpose other than that for which it was originally collected or for a purpose which it was processed by the transferring organization. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon as is practicable, but in any event before the organization uses or discloses such information for a purpose other than that specified above.

CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether and how personal information they provide is used or disclosed to third parties, where such use or disclosure is incompatible with the purpose(s) for which it was originally collected, or subsequently authorized by the individual.[(2)] ~~Where choice is offered concerning disclosures to third parties not subscribing to the safe harbor principles, not subject to the Directive or another adequacy finding, nor bound by written agreement to provide at least the same level of protection as required by the principles, this fact must be made clear when individuals are invited to exercise their choice.~~

For sensitive information, (i.e. personal information specifying[(3)] medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual) they must be given affirmative or explicit (opt in) choice if the information is to be used for a purpose other than those for which it was originally collected or disclosed to any type of third party other than those already notified to the individual, or used or disclosed in a manner other than as subsequently authorized by the individual through the exercise of opt in choice. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

ONWARD TRANSFER: An organization may only disclose personal information to third parties consistent with the principles of notice and choice. Where an organization has not provided choice (because a use is not incompatible with a purpose for which the data was originally collected or which was subsequently authorized by the individual) and the organization wishes to transfer the data to a third party, it may do so if it first either ascertains that the third party subscribes to the principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles. If the organization complies with these requirements, it shall not be held responsible when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations.

SECURITY: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

DATA INTEGRITY: Consistent with the principles, an organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

ACCESS: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

ENFORCEMENT: Effective privacy protection must include mechanisms for assuring compliance with the principles, recourse for individuals to whom the data relate affected by non-compliance with the principles, and consequences for the organization when the principles are not followed. At a minimum, such mechanisms must include (a) readily available and

affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

1. Use of the principles in model contracts has not yet been agreed to by the EC.

2. The EC has general concerns about the choice principle because it believes it offers individuals substantially less control of their data in comparison to the situation in Europe. The EC also does not agree with deletion of the crossed out text. In the US view, that sentence goes beyond what is required by the Directive and for this reason should be deleted. The EC does not agree pointing to the Directive's requirement of informed consent. The US has taken the view that if the EC can demonstrate that the prevailing practice in each Member State is reflected by this sentence, we will include the sentence.

3. The EC would prefer for us to use "revealing" rather than "specifying." The USG concern is that revealing is not clear enough, because it allows so much in the way of inference. Given the 10th Circuit's case on the FCC's rules, it may also raise First Amendment issues. US industry has also argued strongly against "revealing."